# Introducción al Estudio de Algoritmos Criptográficos Livianos

Mg. Jorge Eterovic; Esp. Marcelo Cipriano;

Instituto de Investigación en Ciencia y Tecnología
Dirección de Investigación Vicerrectorado de Investigación y Desarrollo.
Universidad del Salvador.
Lavalle 1854 – C1051AAB -Ciudad Autónoma de Buenos Aires - Argentina

{jorge.eterovic; cipriano1.618}@gmail.com

## RESUMEN

La llamada Internet de las Cosas[1] trata acerca de la conectividad, usando la red Internet, que se realizará entre objetos de diversa naturaleza (tanto en hardware como en software). Los cuales a su vez podrán interconectarse de manera variada y persiguiendo diferentes finalidades. Extendiendo los límites del concepto MtoM[2] (o también M2M).

Las Redes WSN[3] y dispositivos de tipo RFID[4] de manera invisible se suman al ecosistema en el que los seres humanos conviven. Conforman el andamiaje de la IoT, que promete un cambio de paradigma para la humanidad.

Sólo a modo de ejemplo ya existen zapatillas con sensores GPS y conexión Bluetooth, que reciben órdenes de un teléfono móvil conectado a Google Maps[1] pensadas para ayudar a personas invidentes para guiarlos.

Esta nueva era que se vislumbra con el advenimiento de la IoT conlleva consigo un enorme desafío: proteger la información que procesan los dispositivos, que se mueve por las redes y es almacenada en equipos y reservóreos. Muchos de ellos, tal vez, no cuenten con los mecanismos de seguridad adecuados.

Volviendo al ejemplo pero aportando un nuevo punto de vista: ¿Qué consecuencias le podrían acarrear al usuario de las zapatillas que terceras partes tengan acceso a la información de su posición en tiempo real, al recorrido o a su destino? ¿Qué podría ocurrir si se hiciesen cambios no autorizados de los mismos?

Éstas y muchas otras preguntas surgen al realizar un analisis del tipo de información que estos dispositivos procesan. Queda expuesto el impacto desfavorable sobre los usuarios si su información no estuviese protegida por técnicas de confidencialidad, entre otras.

Este proyecto persigue realizar un estudio y análisis de algoritmos criptográficos que podrían ser ejecutados en dispositivos con limitados recursos de hardware y software haciendo uso de Criptografía Ligera[2].

***Palabras Clave:***
*Criptografía Ligera, RFID, Internet de las Cosas, Internet of Things.*

## CONTEXTO

El Vicerrectorado de Investigación y Desarrollo (VRID), perteneciente a la Universidad Nacional del Salvador (USAL), dicta las políticas referidas a la investigación, concibiéndola como un servicio a la comunidad, entendiendo que los nuevos conocimientos son la base de los cambios sociales y productivos. Con el impulso de las propias

[1] Internet of Things: Internet de las Cosas.
[2] Machine to Machine: máquina a máquina. Se refiere la comunicación para el intercambio de información entre dos dispositivos distantes o remotos.
[3] Wireless Sensor Network: Redes Inalámbricas de Sensores.
[4] Radio Frequency Identification: identificación por radiofrecuencia.

Unidades Académicas se han venido desarrollando acciones conducentes a concretar proyectos de investigación uni/multidisciplinarios, asociándolos a la docencia de grado y postgrado y vinculando este accionar, para potenciarlo, con otras instituciones académicas del ámbito nacional e internacional.

La Dirección de Investigación, dependiente del VRID, brinda soporte a las distintas Unidades de Investigación de la y a sus investigadores para el desarollo de Proyectos y Programas de Investigación, nacionales e internacionales, como así también, apoyo y orientación de recursos para la investigación.

A ella pertenece el Instituto de Investigación en Ciencia y Tecnología (RR 576/12) en el cual se enmarca este proyecto, con una duración de 2 años ( 2017-2018).

# 1. INTRODUCCIÓN

El cambio social y cultural que ofrece a la humanidad la llamada IoT promete influir sobre algunos aspectos de la sociedad[3]:

- Cuidados médicos.
  Manufactura de productos.
- Uso de la energía.
- Infraestructura urbana.
- Seguridad
- Extracción de recursos naturales.
- Agricultura
- Ventas
- Vehículos

Sin embargo este cambio está sustentado en dispositivos que por sus características físicas están limitados en el uso de determinados recursos, como son, entre otros:

- Espacio
- Consumo de energía
- Memoria
- Capacidad de cómputo

En el último Ericsson Mobility Reportdel año 2015, el gigante de la telefonía prevee que 28.000.000.000 de teléfonos estarán conectados para el año 2021, más de la mitad de ellos con capacidades de IoT y M2M[4].

Dado que la telefonía móvil incrementará su población actual, se espera que esta demanda de conectividad en aumento sea satisfecha con el advenimiento de la nueva tecnología 5G[5].

Estos dispositivos móviles intercambiarán información con objetos de la vida cotidiana: desde zapatillas con GPS y Bluetooth (como las del ejemplo anterior), heladeras que hacen la lista de los alimentos que faltan y cajones que se abren/cierran automáticamente[5] esta lista sigue incrementándose a diario.

Estos aparatos y los que vendrán tienen en común que la comunicación que establezcan entre ellos debe estar protegida. Volviendo a las zapatillas, es de esperar que su potencia de cómputo sea muy limitada (por el espacio, por ejemplo) y es válido preguntar ¿qué tanto puede hacer para segurizar la información?

La Criptografía Ligera o Liviana estudia algoritmos que por sus propiedades matemáticas pueden ejecutarse en plataformas o dispositivos de recursos limitados, como lo son los que conforman IoT.

Algunos algoritmos son diseñados para ser eficientes en un entorno determinado: hardware o software. Otros en cambio pueden serlo en cualquiera de los dos entornos.

Todas las aplicaciones de la Criptografía tradicional encuentran su par en la Criptografía Liviana. Por ejemplo Block Ciphers[6] y Stream Ciphers[7]. También existen algoritmos de Clave Pública[8].

A modo de ejemplo cabe mencionar que recientemente la agencia[6] gubernamental

[5] 5G: es la llamada 5ta generación de Tecnologías de Telefonía Móvil. Su antecesora, la tecnología 4G aún no del todo difundida en nuestro país.

[6] Algoritmo de Cifrado por Bloques: algoritmos que dividen el mensaje a cifrar en bloques de n bits y luego proceden al cifrado del bloque.

[7] Algoritmo de Cifrado en Cadena o Flujo: algoritmos que generan largas secuencias seudoaleatorias de bits, los cuales uno a uno pueden ser operados con cada bit del mensaje a cifrar.

[8] Algoritmos que utiliza 2 claves, una de ellas es pública y sirve para cifrar el mensaje. La otra permanece secreta y se usa para descifrar el mensaje. También son llamados Algoritmos Asimétricos, por el uso que se hace de sus claves.

NSA[9],ha dado a conocer para uso público, dos algoritmos de cifrado por bloques, llamados SIMON y SPECK[7] que por sus características se enmarcan en Criptografía Liviana y están orientados a hardware y software, respectivamente.

## 2. LÍNEAS DE INVESTIGACIÓN y DESARROLLO

Simon y Speck, como así también muchos otros algoritmos deben demostrar su robustez frente a ataques criptoanalíticos[10]. Profundizar el estudio de sus propiedades criptológicas, matemáticas, hallar vulnerabilidades, debilidades y la búsqueda de posibles claves débiles son objetivos que se propone esta línea de investigación.

Para ello se realizará un relevamiento, estudio y análisis exhaustivo de los principales algoritmos, que podrían ser usados en IoT, poniéndo énfasis en los stream ciphers. Los que por sus características podrían ser empleados por la mayoría de los dispositivos de tipo RFID.

Se definirán indicadores utilizando las experiencias publicadas en trabajos internacionales para evaluar comportamientos y permitir comparaciones entre algoritmos, si ello es posible.

Se volcarán los resultados obtenidos en una tabla comparativa sobre el comportamiento de algoritmos.

Finalmente se redactará un informe final con los resultados obtenidos.

## 3. RESULTADOS OBTENIDOS/ ESPERADOS

El objetivo de este proyecto es abordar y profundizar en el conocimiento de las propiedades criptológicas y de seguridad de Algoritmos Criptográficos Livianos que puedan emplearse en Internet de las Cosas[8] u otros dispositivos semejantes, que así lo requieran por sus limitaciones.

Se realizará un relevamiento exhaustivo de los principales algoritmos criptográficos ligeros existes y determinará cuáles se podrían se implementados en esos dispositivos.

Se definirán indicadores utilizando otras experiencias internacionales para avaluar comportamientos y permitir comparaciones.

## 4. FORMACIÓN DE RECURSOS HUMANOS

El equipo de investigadores pertenece al cuerpo docente de Tecnologías Aplicadas en la Facultad de Ingeniería, el área de la Seguridad Informática, de la Universidad del Salvador.

Dado que este proyecto recién inicia se espera que en breve se sumen a él alumnos de las carrera de Ingeniería en Informática y Licenciatura en Sistemas de Información, que se dictan en la Facultad de Ingeniería.

## 5. BIBLIOGRAFÍA.

[1] http://www.lanacion.com.ar/1753934-las-zapatillas-con-gps-dan-un-primer-paso-buscando-nuevos-mercados. Consultada el 1-3-2017.

[2] ISO/IEC 29192. Information tech-nogy - Security techniques - Lightweight Cryptography. 2012. https://www.iso.org.

[3] Manyika, J.; Chui, M.; Bughin, J.; Dobbs, R.; Bisson, P.; Marrs, A.Disruptive technologies: Advances that will transform life, business, and the global economy. McKinsey Global Institute. 2013.

[4] https://www.ericsson.com/mx/news/2015-11-17-emr-es_254740126_c. Consultada el 1-3-2017.

[5] http://tn.com.ar/tecno/f5/ces-2016-las-heladeras-del-futuro-conectadas-y-con-multiples-sensores_647274

[9] National Security Agency: Agencia de Seguridad Nacional. Organismo gubernamental de Estados Unidos.

[10] Criptoanálisis: parte de la Criptología que se encarga de analizar, estudiar y desarrollar ataques para el descubrimiento de los mensajes cifrados o las claves que fueron empleadas.

[6] http://www.nsa.gov/. Consultada el 1-3-2017.

[7] http://eprint.iacr.org/2013/404.pdf

[8] Masanobu Katagi; Shiho Moriai, Lightweight Cryptography for the Internet of Things; Sony Corporation; 2016.